

Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application.

1. (currently amended) A method for authorizing a transaction, the method comprising:
receiving a request at a wallet server, from a user, for payment authorization, said payment authorization directed to a financial institution;
prompting said user to physically interface a ~~transaction-card-product~~ smartcard with a card reader system;
receiving a digital certificate, read by said card reader system, from said ~~transaction-card-product~~ smartcard wherein said ~~transaction-card-product~~ smartcard includes said digital certificate configured to uniquely identify said smartcard ~~authenticate that said transaction-card-product was physically interfaced with said card reader system;~~
receiving, at a security server, said digital certificate from a computer coupled to said card reader system;
authenticating, by said security server, that said ~~transaction-card-product~~ smartcard was ~~physically interfaced with~~ read by said card reader system;
receiving authorization of said request by said wallet server, from said security server;
associating authentication data, by said wallet server, with a form; and,
providing said form to a merchant server to facilitate the use of said form to obtain an authorization from said security server.
2. (canceled)
3. (currently amended) The method of Claim 1, wherein said request includes purchase information, charge information and ~~transaction-card-product~~ smartcard identifying information.
4. (currently amended) The method of Claim 1, wherein said wallet server is a digital wallet server.

5. (previously presented) The method of Claim 1, wherein said card reader system is a smart card reader system.

Claims 6-38 (canceled).

39. (currently amended) A wallet server for facilitating a transaction, said wallet server including:

an interface configured to receive an authorization request from a user, wherein said request includes a digital certificate from a smartcard ~~transaction card~~, wherein said digital certificate is configured to uniquely identify said smartcard ~~authenticate that said transaction card product was physically interfaced with said card reader system~~;

a processor configured to receive and process said request at said wallet server, and to obtain authentication data from a security server based on said digital certificate; a module configured to associate said authentication data with a form; and,

a module configured to provide said form to a merchant server to facilitate the use of said form to obtain an authorization from said security server.

40. (currently amended) A computer-readable storage medium containing a set of instructions for a general purpose computer, wherein said set of instructions include the steps of:

receiving a request at a wallet server, from a user, for payment authorization, said payment authorization directed to a financial institution;

prompting said user to physically interface a ~~transaction card product~~ smartcard with a card reader system;

receiving a digital certificate, read by said card reader system, from said ~~transaction card product~~ smartcard, wherein said ~~transaction card product~~ smartcard includes said digital certificate configured to uniquely identify said smartcard ~~authenticate that said transaction card product was physically interfaced with said card reader system~~;

receiving, at a security server, said digital certificate from a computer coupled to said card reader system;

authenticating, by said security server, that said ~~transaction card product~~ smartcard was ~~physically interfaced with~~ read by said card reader system;

receiving authorization of said request by said wallet server, from said security server;
associating authentication data, by said wallet server, with a form; and,
providing said form to a merchant server to facilitate the use of said form to obtain an
authorization from said security server.

Claims 41-43 (canceled).